UNITED STATES MARINE CORPS
MARINE CORPS LOGISTICS BASES
814 RADFORD BOULEVARD
ALBANY, GEORGIA 31704-0323

IN REPLY REFER TO:
2000
G600
JUN 1 0 2002

POLICY STATEMENT 6-02

From: Commander
To: Distribution List

Subj: SECURITY CONFIGURATION MANAGEMENT POLICY

Ref: (a) SECNAVINST 5239.3 DON INFOSEC Program (NOTAL)
(b) MARCORLOGBASES Automated Information Systems (AIS) Security Policy
(c) CMC Washington DC// R212006Z May 01, Preparing for Legacy Applications Transition to the Navy Marine Corps Intranet (NMCI) Environment
(d) Directive 5200.28, Security Requirements for Automated Information Systems (AISs)

1. Purpose. To maintain a high level of network security, comply with existing written directives, and establish configuration controls that will lead to the DoD Information Technology Security Certification and Accreditation Process certification and accreditation of Marine Corps Logistics Bases (MARCORLOGBASES) AIS resources as dictated in references (a), (b), (c) and (d).

2. Background. AIS hardware and software configuration controls are critical to the establishment of a secure, certified system and network. Any changes to the network or to the systems attached to the network have the potential of introducing security risks that could be detrimental to the functioning and operation of the command. Similarly, failure to patch or apply security upgrades to AISs would also introduce security risks to the network.

3. Policy. Local Information Technology support sections, i.e., S6/Information Systems Office/Information Systems Management Office, will ensure that all AIS resources as defined in reference (b), which are connected to the local base network, are configured and in compliance with published configuration and security standards. The Assistant Chief of Staff (AC/S) G6 will act as arbitrator when there is a perceived conflict between mission accomplishment and network security.

4. Administrative Actions. Due to the ramifications of a network security breach, failure to comply with this policy could compromise Local Area Networks, data integrity, overall security of the Marine Corps Enterprise Network, and may prevent the migration of the system or application to NMCI. Systems or applications determined to be in non-compliance will be required to take immediate corrective action to comply with this policy and to obtain an Interim Authority To Operate from the Marine Corps Information Technology and Network Operations Center.

5. Point of Contact. Address questions concerning Information Assurance to MARCORLOGBASES AC/S, Information Technology Department, Information Assurance Office (G620) at DSN 567-7133 or Commercial (229)-639-7133. Email is matcomg6iaoffice@matcom.usmc.mil. Information can also be obtained from the MARCORLOGBASES G6 Information Assurance Office website at http://www.ala.usmc.mil/iao.

6. Applicability. This policy is applicable to organic and tenant activities aboard Marine Corps Logistics Base (MCLB) Albany, MCLB Barstow, and Blount Island Command.

RS Kramlich
R. S. KRAMLICH

Distribution: A